

**RECEIVED  
CENTRAL FAX CENTER**

**OCT 03 2005**

PTO/SB/21 (09-04)

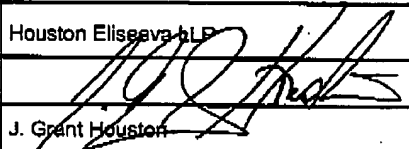
Approved for use through 07/31/2008. OMB 0651-0031

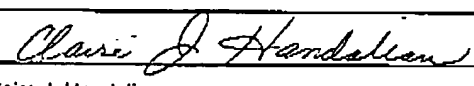
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>TRANSMITTAL FORM</b>  (to be used for all correspondence after initial filing)	Application Number	09/777,550	
	Filing Date	February 5, 2001	
	First Named Inventor	David J. Wetherall	
	Art Unit	2151	
	Examiner Name	Phillips, Hassan A.	
Total Number of Pages in This Submission	25	Attorney Docket Number	0016.0006

ENCLOSURES (Check all that apply)		
<input checked="" type="checkbox"/> Fee Transmittal Form <input type="checkbox"/> Fee Attached <input type="checkbox"/> Amendment/Reply <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/declaration(s) <input checked="" type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input type="checkbox"/> Information Disclosure Statement <input type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Reply to Missing Parts/Incomplete Application <input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert to a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation <input type="checkbox"/> Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s) _____ <input type="checkbox"/> Landscape Table on CD	<input type="checkbox"/> After Allowance Communication to TC <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input checked="" type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input type="checkbox"/> Other Enclosure(s) (please identify below):
Remarks <span style="float: right;"><b>RECEIVED OIPE/IAP OCT 04 2005</b></span>		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT			
Firm Name	Houston Eliseeva LLP		
Signature			
Printed name	J. Grant Houston		
Date	October 3, 2005	Reg. No.	35,900

CERTIFICATE OF TRANSMISSION/MAILING			
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:			
Signature			
Typed or printed name	Claire J. Handal	Date	October 3, 2005

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

**RECEIVED**  
**CENTRAL FAX CENTER**

**OCT 03 2005**

PTO/SB/17 (12-04v2)

Approved for use through 07/31/2006. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Effective on 12/08/2004.  
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4618).

# **FEE TRANSMITTAL**

## **For FY 2005**

☒ Applicant claims small entity status. See 37 CFR 1.27

**TOTAL AMOUNT OF PAYMENT** (\$) 760.00
**Complete if Known**

Application Number	09/777,550
Filing Date	February 5, 2001
First Named Inventor	David J. Wetherall
Examiner Name	2151
Art Unit	Phillips, Hassan A.
Attorney Docket No.	0016.0006

**METHOD OF PAYMENT** (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): \_\_\_\_\_

☒ Deposit Account Deposit Account Number: 502233 Deposit Account Name: Houston Eliseeva LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☒ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☒ Credit any overpayments

**WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

**FEE CALCULATION****1. BASIC FILING, SEARCH, AND EXAMINATION FEES**

Application Type	FILING FEES		SEARCH FEES		EXAMINATION FEES		Fees Paid (\$)
	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

**2. EXCESS CLAIM FEES****Fee Description**

Each claim over 20 (including Reissues)

Each independent claim over 3 (including Reissues)

Multiple dependent claims

Fee (\$)	Small Entity Fee (\$)
50	25
200	100
360	180
Multiple Dependent Claims	
Fee (\$)	Fee Paid (\$)

<b>Total Claims</b>	<b>Extra Claims</b>	<b>Fee (\$)</b>	<b>Fee Paid (\$)</b>
---------------------	---------------------	-----------------	----------------------

- 20 or HP = \_\_\_\_\_ x \_\_\_\_\_ = \_\_\_\_\_

HP = highest number of total claims paid for, if greater than 20.

<b>Indep. Claims</b>	<b>Extra Claims</b>	<b>Fee (\$)</b>	<b>Fee Paid (\$)</b>
----------------------	---------------------	-----------------	----------------------

- 3 or HP = \_\_\_\_\_ x \_\_\_\_\_ = \_\_\_\_\_

HP = highest number of independent claims paid for, if greater than 3.

**3. APPLICATION SIZE FEE**

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

<b>Total Sheets</b>	<b>Extra Sheets</b>	<b>Number of each additional 50 or fraction thereof</b>	<b>Fee (\$)</b>	<b>Fee Paid (\$)</b>
---------------------	---------------------	---	-----------------	----------------------

- 100 = \_\_\_\_\_ / 50 = \_\_\_\_\_ (round up to a whole number) x \_\_\_\_\_ = \_\_\_\_\_

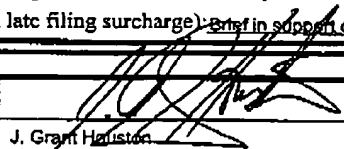
**4. OTHER FEE(S)**

Non-English Specification, \$130 fee (no small entity discount)

Other (e.g., late filing surcharge): brief in support of Appeal (\$250) and 3 month extension fee (\$10)**Fees Paid (\$)**

760.00

**SUBMITTED BY**

Signature		Registration No. (Attorney/Agent)	35,900	Telephone	781-863-9991
Name (Print/Type)	J. Grant Houston			Date	October 3, 2005

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

RECEIVED  
CENTRAL FAX CENTER

OCT 03 2005

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re: David J. Wetherall Confirmation No: 8207  
Serial No: 09/777,550 Group: 2151  
Filed: February 5, 2001 Examiner: Phillips,  
Hassan A.  
For: Network Traffic Regulation  
Including Consistency Based  
Detection and Filtering of Packets  
with Spoof Service Addresses  
Customer No.: 29127  
Attorney 0016.0006US1  
Docket No.

APPELLANT'S BRIEF

VIA FACSIMILE: 571-273-8300  
Mail Stop Appeal Brief- Patents  
Commissioner for Patents  
P.O. Box 1450,  
Alexandria, Virginia 22313-1450

Sir:

This is the Applicants' appeal from the final Office Action, mailed December 2, 2004 (Paper No.20040806).

A three-month extension is requested for this response.

**Real Party in Interest**

Arbor Networks, Inc. is the real party of interest.

**Related Appeals and Interferences**

There are no related appeals or interferences.

10/04/2005 HDEMESS1 00000075 502233 09777550

01 FC:2402 250.00 DA

10/04/2005 HDEMESS1 00000075 502233 09777550

02 FC:2253 510.00 DA

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

### **Status of Claims**

Claims 1-34 and 36-48 are pending. Claims 1-34 and 36-48 are rejected.

### **Status of Amendments**

All amendments have been entered. There were no post final amendments or proposed amendments.

### **Summary of Claimed Subject Matter**

The present invention is directed to a network or a networking method. Fig. 1 illustrates the basic architecture of an embodiment. A director 102 communicates with a number of sensors 104a, 104b, which communicate with routing devices 106a-106e. These routing devices move network traffic between clients 108a, 108b and servers 110 of the various network domains.

The present invention is capable of protecting this network 100 from packets having spoofed source addresses. A packet with a spoofed source address would be a packet that originated from a place other than that indicated by its source address. Such spoofed packets are often used in attacks on networks since these malformed packets will hide the actual original of the attack.

The invention detects the spoof source addresses using "consistency measures."

In one example, the determination of whether the source addresses are spoofed is based upon spatial distribution profiles of the source addresses of the packets (claim 2). Spatial distribution refers to how the packets are distributed in the network and routed through the network relative to their source addresses. For example, a source address may have historically taken one path had a given distribution through the network, but if similar source addresses were now taking a new path or have a new distribution through the network, this would indicate a new spatial distribution.

In another example, spoofed source addresses are determined based on a source address range distribution profile (claim 4). This refers to a comparison of the range of destination and source addresses. As described in the present application relative to Fig.

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

14a, spoofed source addresses tend to be a subset or substantially related to source addresses of other packets being routed to other destinations at a routing location.

In another example, spoof source addresses are identified based on migration distribution profiles (claim 6). Migration profiles address the rapidity with which the routing paths change for the reported source addresses.

In another example, spool source addresses are identified based on timing distribution profiles (claim 8). Timing distribution profiles address the rapidity with which packets with the reported source address are issued. For example, if one source address is issuing packets very quickly, this could be used to determine that those packets had spoofed source addresses

Once identified, the network can then determine a response to the spoofed source addresses. In one example, the director determines filtering actions to be taken to remove the spoofed packets and how to distribute those filtering actions among the routing devices.

### **Grounds of Rejection to be Reviewed on Appeal**

Whether claims 2-14, 16-34, and 36-48 are anticipated by Porras *et al.*, U.S. Patent 6,321,338 (hereinafter Porras patent).

### **Argument**

#### Concerning claims 1 and 15

Arguments concerning the non-anticipation of claims 1 and 15 are not being presented. Further review of the Porras patent in the preparation of this Brief revealed the description of the first full paragraph in column 14 of the Porras patent. This paragraph mentions the use of long-term and short-term statistical profiles for a satellite office to detect "address spoofing."

#### Non-anticipation of claim 2

Claim 2 requires that the determination of whether routed packets have spoofed source addresses is made based upon spatial distribution profiles. As mentioned

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

previously, a spatial distribution profile characterizes how source addresses are distributed over the network domain. For example, it would be expected that a given network domain would transport a large number of packets with source addresses for sources located within that network domain.

This method for detecting spoofed source addresses is not shown in the Porras patent. Thus, Applicant believes that the rejection of this claim should be withdrawn.

The pending Office Action argues that the functionality of claim 2 is described at column 5, lines 36-51 of the Porras patent. This portion of the Porras patent, however, merely provides that the Porras profile engine 22 uses statistical measures to characterize patterns of usage. In contradistinction, the Porras patent does not suggest that spoofed source addresses should be determined based on spatial distribution profiles as claimed. Thus, there is no anticipation.

Non-anticipation of claim 16

Similar to claim 2, claim 16 is also directed to the use of spatial distribution profiles in the detection of spoof instances of source addresses, but in the context of a networking method. It is thus is patentable for reasons similar to those set forth relative to claim 2 above. In short, the Porras patent does not suggest a method using spatial distribution profiles.

Non-anticipation of claim 34

Similar to claim 2, claim 34 is also directed to the use of spatial distribution profiles in the detection of spoof instances of source addresses, but in the context of an apparatus. It is thus is patentable for reasons similar to those set forth relative to claim 2 above. In short, the Porras patent does not suggest an apparatus using spatial distribution profiles.

Non-anticipation of claim 3

Claim 3, dependent on claim 2, further characterized the spatial distribution profile by specifying that this profile comprises an exemplary spatial distribution profile

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

for non-spoofed addresses and/or an historical spatial distribution profile for a particular address.

The Porras patent fails to describe something akin to the claimed spatial distribution profile for spoofed address detection. It moreover fails to so specify such a profile as comprising exemplary or historical profiles. Thus there is no anticipation here.

The pending Office Action identifies column 5, lines 38-40 as disclosing the features of this claim. This portion of the Porras patent only describes the profile engine 22 and its keeping of statistical scores. In contradistinction, it does not teach that the existence of a spoofed source address can be determined based upon a spatial distribution profile that comprises an exemplary spatial distribution profile or an historical spatial distribution profile as claimed in claim 3. Thus, there is no anticipation.

#### Non-anticipation of claims 17 and 36

Claim 17 is also directed to the construction of spatial distribution profiles in the detection of spoof instances of source addresses, but in the context of a networking method. Claim 36 is directed to the apparatus. They are thus patentable for reasons similar to those set forth relative to claim 3 above. In short, the Porras patent does not suggest a method or apparatus with the claimed spatial distribution profiles.

#### Non-anticipation of claims 18 and 37

Claim 18, depending from 16, is directed to the determining of whether each of the spatial distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address spatial distribution profile in the detection of spoof instances of source addresses, but in the context of a networking method. Claim 37 is directed to the apparatus. They are thus patentable for reasons similar to those set forth relative to claim 3 above and in further view that the Porras patent does not suggest such resemblance tolerances.

#### Non-anticipation of claim 19

Claim 19 is also directed to the fact that the reference spatial distribution profile comprises at least a selected one of an exemplary spatial distribution profile for a non-

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

spoof source address in general and a historical spatial distribution profile for a particular source address, but in the context of a networking method. It is thus is patentable for reasons similar to those set forth relative to claim 3 above.

#### Non-anticipation of claim 4

Claim 4 provides that the director determines whether a packet has a spoofed source address based on a destination source address range distribution profile. Destination source address range profiles are measures of source address ranges of other packets being routed to other destinations at a reporting location. This is not shown by the Porras patent. Porras fails to mention such a profile type or its usage in spoof source address packet identification. Thus there is no anticipation.

The Office Action argues that the subject matter of claim 4 is taught at column 5, lines 36-51 of the Porras patent. This portion of the Porras patent, however, describes a profile engine that uses statistical scores to identify anomalous events. Measures include categorical, continuous, intensity, and distribution measures. Nonetheless, this portion of the Porras patent does not show or suggest that packets having spoofed source addresses should be identified based on destination source address range distribution profiles as claimed.

#### Non-anticipation of claim 20

Similar to claim 4, claim 20 is also directed to the use of destination source address range (DSAR) distribution profiles in the detection of spoof instances of source addresses, but in the context of a networking method. It is thus is patentable for reasons similar to those set forth relative to claim 4 above, the Porras patent not providing for such a method.

#### Non-anticipation of claims 21 and 39

Claim 21 is further directed to the construction of the DSAR distribution profiles of the source addresses. Claim 39 is directed to the apparatus. They are thus further patentable relative to claim 20 above.

#### Non-anticipation of claims 22 and 40



3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

Claim 22 includes the determination of whether DSAR distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address DSAR distribution profile. Claim 40 is directed to the apparatus. They are thus further characterizes the method of claim 20 and is thus further patentable. The Porras patent does not disclose such details.

Non-anticipation of claim 38

Similar to claim 4, claim 38 is also directed to the use of destination source address range (DSAR) distribution profiles in the detection of spoof instances of source addresses, but in the context of an apparatus. It is thus is patentable for reasons similar to those set forth relative to claim 4 above.

Non-anticipation of claim 5

Claim 5, depending on claim 4, further requires that the source address range distribution profile comprises an exemplary distribution profile for non-spoofed source addresses or an historical profile. It therefore further characterizes the profile definition set forth in claim 4. The Porras patent fails to provide for such a source address range distribution profile, in any context much less spoof address detection. It further fails to set forth that such a profile should include such exemplary or historical profiles.

The present Office Action identifies column 5, lines 38-40 of the Porras patent for the disclosure of the feature of claim 5. That portion of the Porras patent does not suggest that packets having spoofed source addresses should be identified based on source address range distribution profiles or that such profiles should be based on exemplary distribution profiles or historical distribution profiles as claimed. Instead, this portion of the Porras patent provides a general description of a profile engine, but does not provide for the specific claimed profile of claim 5.

Non-anticipation of claim 23

Similar to claim 5, claim 23 is also directed to the fact that one reference DSAR distribution profile comprises at least a selected one of an exemplary DSAR distribution profile for a non-spoof source address in general, and a historical DSAR distribution

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

profile for a particular source address, but in the context of a networking method. It is thus is patentable for reasons similar to those set forth relative to claim 5 above.

Non-anticipation of claim 6

Claim 6 requires that the director determines whether packets have spoofed source addresses based on migration distribution profiles for those source addresses that are based at least in part a reference migration distribution profile. Migration profiles address the rapidity with which routing paths change for the reported source addresses. The Porras patent fails to suggest that address spoofing may be identified based on migration information or such information should even be collected for spoofing detection. Therefore, there is no anticipation.

The pending Office Action points to the Porras patent at column 5, lines 36-51 as anticipating the subject matter of claim 6. This portion of the Porras patent concerns the description of the profile engine 22. This profile engine develops statistical scores that characterize how current usage compares with historical usage. However, this portion of the Porras patent does not teach that spoofed addresses should be identified based on migration distribution profiles, and in fact does not even mention migration profiles.

Non-anticipation of claim 24

Similar to claim 6, claim 24 is also directed to the use of migration distribution profiles in the detection of spoof instances of source addresses, but in the context of a networking method. It is thus is patentable for reasons similar to those set forth relative to claim 6 above, and in view of the fact that the Porras patent does not disclose such a method.

Non-anticipation of claim 41

Similar to claim 6, claim 41 is also directed to the use of migration distribution profiles in the detection of spoof instances of source addresses, but in the context of an apparatus. It is thus is patentable for reasons similar to those set forth relative to claim 6 above.

Non-anticipation of claims 25 and claim 42

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

Claim 25 further adds to claim 24 that the determining step includes the construction of the migration distribution profiles of the source addresses. Claim 42 is similar, but directed to the apparatus. In contradistinction, the Porras patent does not provide for the construction of these profiles especially in the context of spoof address detection. Thus, this claim is further patentable.

Non-anticipation of claims 26 and 43

Claim 26 adds to claim 24 that the determination of the spoof addresses by determining whether the each of the migration distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address migration distribution profile. Claim 43 is similar but directed to the apparatus. The Porras patent does not provide for such application of these profiles in the context of spoof address detection. Thus, these claims are further patentable.

Non-anticipation of claim 7

Claim 7, depending from claim 6, requires that the migration distribution profiles comprise exemplary migration distribution profile for non-spoofed source addresses or an historical migration distribution profile for a particular source address. This is not suggested by the Porras patent, which does not teach spoofed source addresses should be identified based on migration distribution profiles or that such profiles should comprise exemplary migration distribution profiles or historical migration distribution profiles as claimed. Thus, for these additional reasons, this claim is not anticipated.

The pending Office Action cites to column 5, lines 38 of the Porras patent as disclosing the subject matter of claim 7. As discussed previously, however, this portion of the Porras patent merely describes the profile engine 22 in the Porras system. While using statistical scores to characterize current versus established usage patterns, it does not show or suggest that spoofed source addresses should be identified using this claimed migration distribution profile or a profile constructed as specified by claim 7.

Non-anticipation of claim 27

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

Similar to claim 7, claim 27 is also directed to the fact that comprises at least a selected one of an exemplary migration distribution profile for a non-spoof source address in general, and a historical migration distribution profile for a particular source address., but in the context of a networking method. It is thus is patentable for reasons similar to those set forth relative to claim 7 above.

Non-anticipation of claim 8

Claim 8 requires that the detector bases its determination of whether a packet has a spoofed source address or not using timing distribution profiles for the packets and in view of at least one reference source timing distribution profile. Timing distribution profiles address the rapidity with which packets with the reported source addresses are issued. The Porras patent does not teach that spoofed source addresses should be identified using this technique. Thus, there is no anticipation.

The pending Office Action argues that the Porras patent at column 5, lines 36-51 teaches the features of this claim. This portion of the Porras patent, however, concerns the description of a profile engine 22 that uses statistical scores to characterize current versus established patterns of usage. The engine profiles network activity using one or more variables such as categorical, continuous, intensity, and event distribution measures. This portion of the Porras patent, however, does not show or suggest that spoofed source addresses should be identified based on timing distribution profiles as claimed. In fact, it completely fails to mention spoofed addresses much less using such a profile for identifying such addresses.

Non-anticipation of claims 28 and 44

Similar to claim 8, claim 28 is also directed to the use of timing distribution profiles in the detection of spoof instances of source addresses, but in the context of a networking method. Claim 44 concerns the apparatus. They are thus is patentable for reasons similar to those set forth relative to claim 8 above.

Non-anticipation of claims 29 and 45

3 October 2005  
Application No.: 09/777,550  
Docket: 0016:0006us

Claim 29 is also directed to the construction of timing distribution profiles in the detection of spoof instances of source addresses, but in the context of a networking method. Claim 44 is directed to the apparatus. They are thus is patentable for reasons similar to those set forth relative to claim 8 above.

Non-anticipation of claims 30 and 46

Claim 30 is directed to the determining of whether each of the timing distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address timing profile in the detection of spoof instances of source addresses, but in the context of a networking method. Claim 46 is directed to the apparatus. They are thus is patentable for reasons similar to those set forth relative to claim 8 above.

Non-anticipation of claim 9

Claim 9, depending from claim 8, further requires that the timing distribution profiles that are used to identify packet with spoofed source addresses should comprise an exemplary timing distribution profile for non-spoofed source addresses or an historical timing distribution profile for a particular source address. The Porras patent does not teach that spoofed source addresses should be identified based on these types of timing distribution profiles or that the profiles should be defined as claimed. Thus there is no anticipation.

The pending Office Action argues that the subject matter of claim 9 is shown in the Porras patent at column 5, lines 38-40. This portion of the Porras patent, however, merely describes the profile engine 22 and the profile engine only in very general terms. It sets forth that how the profile engine uses statistical scores as a metric for characterizing how closely current usage corresponds to established usage patterns but not the claimed profile or that this claimed profile should be used for spoofed source address detection. Moreover, it does not show or suggest that timing distribution profiles having exemplary distribution profiles or historical timing profiles should be used to identify packets with spoofed source address.

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

Non-anticipation of claim 10

Claim 10 requires that the director is equipped to determine whether filtering actions are to be taken to filter out packets with source addresses that are deemed to be spoofed source addresses and further how those filtering actions should be distributed among the routing devices.

Attorney for Applicant has closely reviewed the applied Porras patent. It is believed that the Porras patent does not show that such determinations should be used to initiate filtering actions at the routing devices as claimed. That is, the Porras patent is primarily directed to how a system identifies anomalous or events or suspicious activity and then further reconfigures itself to further analyze that specific activity. It is designed to characterize anomalous events. However, it does not seek to control the underlying network, to insulate it from those same anomalous events. In short, the Porras system does not respond to anomalous events other than to further analyze and report those events. Applicants thus believe that claim 10 is not anticipated.

Nonetheless, the portions of the Porras patent cited as anticipating claim 10 certainly fail to show the claimed features. For example, the pending Office Action argues that the Porras patent shows packet filtering at column 9, lines 57-63 of the Porras patent. This portion of the Porras patent describes the resolver 20, which is described as issuing intrusion or suspicion reports. Further, it describes how the analysis engines may be reconfigured to change "the collection method's filtering semantics when necessary." See column 9 at lines 62 and 63 of the Porras patent. As indicated previously, this portion of the Porras patent merely states that the analysis engines may be reconfigured in order to collect different information from the events that they are monitoring. For example, in response to a suspicious event such as a large number of packets from a given source address, the analysis engines may be reconfigured to collect further statistics with those source addresses, for example. In contradistinction, this portion of the Porras patent does not show or suggest that packets should be filtered out by the routing devices and the filtering actions by those routing devices. In summary, the Porras patent does not teach that routing devices should be removing packets based on determined suspicious activity as claimed. Thus, there is no anticipation.

3 October 2005  
Application No.: 09/777,550  
Docket: 0016,0006us

Non-anticipation of claim 11

Claim 11, depending from claim 10, further requires that the director takes into consideration in making its determination whether filtering actions should be taken based on where packets of non-spoofed instances of source addresses having instances deemed to be spoofed source addresses are likely to be routed in the network. This refers to making decisions based on how packets propagate through the network. This is not shown by the Porras patent. As noted, the Porras patent simply changes its monitoring of packet, not how the packets are routed as claimed. Moreover, it is certainly not shown by column 10, lines 57-63 which was cited by the pending Office Action as showing this feature.

For the foregoing reasons, Applicants believe that the pending rejections should be withdrawn, and that the present application should be passed to issue. Should any questions arise, please contact the undersigned.

Respectfully submitted,

Houston Eliseeva LLP

By 

J. Grant Houston  
Registration No.: 35,900  
4 Militia Drive, Ste. 4  
Lexington, MA 02421  
Tel.: 781-863-9991  
Fax: 781-863-9931

Date: October 3, 2005

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

## Claims Appendix

1. (Original) A network comprising:
  - a plurality of network nodes;
  - a plurality of routing devices to route network traffics between selected ones of said network nodes; and
  - director coupled to said routing devices to determine whether selected instances of source addresses of packets routed by said routing devices are spoof source addresses, based at least in part on one or more consistency measures.
2. (Original) The network of claim 1, wherein the director bases said determination on at least spatial distribution profiles of said source addresses, and in view of at least one reference source address spatial distribution profile.
3. (Original) The network of claim 2, wherein said at least one reference source address spatial distribution profile comprises at least a selected one of an exemplary spatial distribution profile for a non-spoof source address in general, and a historical spatial distribution profile for a particular source address.
4. (Original) The network of claim 1, wherein the director bases said determination on at least destination source address range (DSAR) distribution profiles of said source addresses, and in view of at least one reference DSAR distribution profile.
5. (Original) The network of claim 4, wherein said at least one reference DSAR distribution profile comprises at least a selected one of an exemplary DSAR distribution profile for a non-spoof source address in general, and a historical DSAR distribution profile for a particular source address.
6. (Original) The network of claim 1, wherein the director bases said determination on at least migration distribution profiles of said source addresses, and in view of at least one reference migration distribution profile.



3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

7. (Original) The network of claim 6, wherein said at least one reference migration distribution profile comprises at least a selected one of an exemplary migration distribution profile for a non-spoof source address in general, and a historical migration distribution profile for a particular source address.
8. (Original) The network of claim 1, wherein the director bases said determination on at least timing distribution profiles of said source addresses, and in view of at least one reference source address timing distribution profile.
9. (Original) The network of claim 8, wherein said at least one reference source address timing distribution profile comprises at least a selected one of an exemplary timing distribution profile for a non-spoof source address in general, and a historical timing distribution profile for a particular source address.
10. (Original) The network of claim 1, wherein the director is further equipped to determine whether filtering actions are to be taken to filter out packets with source addresses having instances deemed to be spoof source addresses, and if filtering actions are to be taken, where among said routing devices, said filtering actions are to be taken.
11. (Original) The network of claim 10, wherein the director takes into consideration in making said where determination, where packets of non-spoof instances of a source address having instances deemed to be spoof source addresses are likely to be routed in said network.
12. (Original) The network of claim 1, wherein the director comprises a plurality of director devices cooperatively coupled to each other to jointly make said determination.
13. (Original) The network of claim 1, wherein the network further comprises a plurality of sensors, either integrally disposed in a subset of said routing devices or externally

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

disposed and coupled to the subset of routing devices, to monitor and report on source addresses of packets routed through the subset of routing devices.

14. (Original) The network of claim 13, wherein the sensors are further equipped to facilitate application of desired source address based filtering on packets being routed through selected ones of said subset of routing devices.

15. (Original) A networking method comprising:

receiving information associated with source addresses of packets being routed to and from a plurality of network nodes of a network;

determining whether selected instances of said source addresses are spoof instances of said source addresses, based at least in part on one or more consistency measures; and

managing said network based at least in part on the results of said determination.

16. (Original) The method of claim 15, wherein said determination is made based at least in part on spatial distribution profiles of said source addresses, and in view of at least one reference source address spatial distribution profile.

17. (Previously presented) The method of claim 16, wherein said determination comprises constructing said spatial distribution profiles of said source addresses.

18. (Original) The method of claim 16, wherein said determining comprises determining whether each of the spatial distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address spatial distribution profile.

19. (Original) The method of claim 16, wherein said at least one reference spatial distribution profile comprises at least a selected one of an exemplary spatial distribution profile for a non-spoof source address in general, and a historical spatial distribution profile for a particular source address.

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

20. (Original) The method of claim 15, wherein said determination is made based at least in part on destination source address range (DSAR) distribution profiles of said source addresses, and in view of at least one reference DSAR distribution profile.
21. (Previously presented) The method of claim 20, wherein said determination comprises constructing said DSAR distribution profiles of said source addresses.
22. (Original) The method of claim 20, wherein said determining comprises determining whether each of the DSAR distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address DSAR distribution profile.
23. (Original) The method of claim 20, wherein said at least one reference DSAR distribution profile comprises at least a selected one of an exemplary DSAR distribution profile for a non-spoof source address in general, and a historical DSAR distribution profile for a particular source address.
24. (Original) The method of claim 15, wherein said determination is made based at least in part on migration distribution profiles of said source addresses, and in view of at least one reference migration distribution profile.
25. (Original) The method of claim 24, wherein said determining comprises constructing said migration distribution profiles of said source addresses.
26. (Original) The method of claim 24, wherein said determining comprises determining whether each of the migration distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address migration distribution profile.

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

27. (Original) The method of claim 24, wherein said at least one reference migration distribution profile comprises at least a selected one of an exemplary migration distribution profile for a non-spoof source address in general, and a historical migration distribution profile for a particular source address.

28. (Original) The method of claim 15, wherein said determination is made based on at least timing distribution profiles of said source addresses, and in view of at least one reference source address timing distribution profile.

29. (Original) The method of claim 28, wherein said determining comprises constructing said timing distribution profiles of said source addresses.

30. (Original) The method of claim 28, wherein said determining comprises determining whether each of the timing distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address timing distribution profile.

31. (Original) The method of claim 28, wherein said at least one reference timing distribution profile comprises at least a selected one of an exemplary timing distribution profile for a non-spoof source address in general, and a historical timing distribution profile for a particular source address.

32. (Original) The method of claim 15, wherein said managing comprises determining whether filtering actions are to be taken in said network to filter out at least some packets having source addresses deemed to be having spoof instances, and if filtering actions are to be taken, where among a plurality of routing devices, said filtering actions are to be taken.

33. (Original) The method of claim 32, wherein said where determination comprises taking into consideration where packets of non-spoof instances of a source address

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

having instances deemed to be spoof source addresses are likely to be routed in said network.

34. (Previously presented) An apparatus comprising:

(a) a storage medium having stored therein a plurality of programming instructions designed to implement a director to receive reporting of information associated with source addresses of packets routed through a plurality of routing devices of a network, and to determine whether at least some instances of said source addresses are spoof instances based on at least spatial distribution profiles of said source addresses, and in view of at least one reference source address spatial distribution profile; and

(b) a processor coupled the storage medium to execute the programming instructions.

35. (Cancelled)

36. (Previously presented) The apparatus of claim 34, wherein said programming instructions are designed to be able to construct said spatial distribution profiles of said source addresses.

37. (Previously presented) The apparatus of claim 34, wherein said programming instructions are designed to be able to determine whether each of the spatial distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address spatial distribution profile.

38. (Original) The apparatus of claim 34, wherein said programming instructions are designed to make said determination based on at least destination source address range (DSAR) distribution profiles of said source addresses, and in view of at least one reference source address DSAR distribution profile.

39. (Original) The apparatus of claim 38, wherein said programming instructions are designed to be able to construct said DSAR distribution profiles of said source addresses.

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

40. (Original) The apparatus of claim 38, wherein said programming instructions are designed to be able to determine whether each of the DSAR distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address DSAR distribution profile.

41. (Original) The apparatus of claim 34, wherein said programming instructions are designed to make said determination based on at least migration distribution profiles of said source addresses, and in view of at least one reference source address migration distribution profile.

42. (Original) The apparatus of claim 41, wherein said programming instructions are designed to be able to construct said migration distribution profiles of said source addresses.

43. (Original) The apparatus of claim 41, wherein said programming instructions are designed to be able to determine whether each of the migration distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address migration distribution profile.

44. (Original) The apparatus of claim 34, wherein said programming instructions are designed to make said determination based on at least timing distribution profiles of said source addresses, and in view of at least one reference source address timing distribution profile.

45. (Original) The apparatus of claim 44, wherein said programming instructions are designed to be able to construct said timing distribution profiles of said source addresses.

46. (Original) The apparatus of claim 44, wherein said programming instructions are designed to be able to determine whether each of the timing distribution profiles of the

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address timing distribution profile.

47. (Original) The apparatus of claim 34, wherein said programming instructions are designed to be able to determine whether filtering actions are to be taken in said network to filter out at least some packets having source addresses deemed to be having spoof instances, and if filtering actions are to be taken, further determine where among a plurality of routing devices, said filtering actions are to be taken.

48. (Original) The apparatus of claim 47, wherein said programming instructions are designed to take into consideration where packets of non-spoof instances of a source address having instances deemed to be spoof source addresses are likely to be routed in said network, when making said where determination.

3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

**Evidence Appendix**

None



3 October 2005  
Application No.: 09/777,550  
Docket: 0016.0006us

**Related proceedings appendix**

None